結合RFID之高速公路電子收費的認證與隱私權保護系統

Constructing a RFID-Combined Authentication and Privacy Protected ETC system

葉禾田、黃翊豪
南台科技大學資訊傳播系
南台街1號
台南市710永康區
htyeh@mail.stust.edu.tw

Her-Tyan Yeh, Yi-Hao Huang
Dept. of Information and Communication, Southern Taiwan University of Science and Technology
No. 1, Nan-Tai Street, Yungkang Dist.,
710 Tainan, Taiwan
htyeh@mail.stust.edu.tw

摘要

資訊科技的跨領域結合應用是現今的潮流。近年來，無線射頻辨識系統（Radio Frequency Identification，以下簡稱RFID）發展快速，以RFID 結合電子收費更是目前及未來發展的一大趨勢。目前國內高速公路仍是以人工收費爲主，車輛進出收費站時容易因時間延宕造成塞車或人爲疏忽，造成駕駛人的不便，即每經過收費站就進行一次收費，此收費方式對大多數駕駛人較爲不公平。基於使用者付費在行駛里程數與人工收費效益不佳的缺點，本研究以RFID 系統與無線網路結合後端資料庫建立自動化系統，架構出一套具備交易安全性、使用便利性、付費公平性之高速公路電子收費的認證與隱私權保護系統。

此系統不僅具備個人隱私保護及資料安全之特性，駕駛人在上路前不必事先花費時間購買回數票或將易通卡儲值，整個電子交易過程可以有效且清楚的記錄駕駛人交易資料，並將費用以月結的方式結合於每月的行動通訊裝置帳單。

關鍵詞: RFID、電子收費系統、行蹤隱私、認證。

Abstract

Cross-integration application for information technologies is nowadays tide. In recent years, radio frequency identification, known as RFID, has been rapidly developed, and it is a trend that combine electronic toll collection and RFID in future advancement. The domestic highway was still by the manual charge. The vehicles waste more time to pass the toll station because the probable traffic jam, and it is inconvenient for the drivers. Besides, the charge is unfair for most drivers by how many toll stations passed. To improve this low efficiency, this study combines RFID system and wireless network to construct a secure, easy to use, and pay fair automatic electronic toll collection system.

This system not only can protect personal privacy and secure data. The driver doesn't need to buy toll tickets or pre-paid cards in advance. All transaction data can be effectively and clearly recorded and charged by the monthly with mobile device bill.

Keywords: RFID、Electronic Toll Collection System、Location Privacy、Authentication

一、緒論

1. 前言

目前台灣的電子收費系統ETC可分爲前端與後端兩類系統，前端系統包含：車道系統、扣款系統、執法系統與車載設備單元(IC卡)。後端系統包含：帳款稽核系統、加值系統與IC卡管理系統。前端車道系統與車載設備單元利用紅外線進行通信，對來往車輛進行判別與資料收集，透過網路將資料傳送至後端管理中心，進行數據儲存及處理與結算等，完成收費程序。駕駛者使用高速公路電子收費車道之前必須預先在儲值卡中儲存足夠的扣款金額以供實際使用扣款之用，此收費方式稱之爲預付方式。傳統電子收費必須在固定的收費匝道進行付費，在收費匝道(ETC與人工收費)的區域易造成塞車問題，因車輛必須減速來進行付款的動作，導致車流速度緩慢，且無法計算出車流量。以上兩種爲目前高速公路收費方式，車輛容易在收費站前產生延滯情況。

隨著RFID技術的發展與各領域上的運用越趨成熟，應用層面也越趨廣泛，RFID技術幾種常見應用領域包含人員身分辨識、門禁管理、物品追蹤、圖書管理系統、車輛辨識、製造業與電子收費系統等[1][2][3]。RFID技術是將標籤裝置在物品上，用來記錄該物品相關資料，Reader可以在任何角度讀取資料及同時讀取多張Tag爲最大優點，並擁有隨時更新資料的特性。RFID系統是一種非接觸式的自動辨識系統，運作原理是經由無線電波傳送通訊資料，在開放式空間可一次讀取多個電子標籤的特點，解決了傳統條碼須以掃描器近距離的一對一掃描的限制。當標籤被用來管理人身資料時，就會產生個人隱私權相關問題。由於RFID資料的傳送方式是經由無線電波進行傳輸，容易被有心人士進行惡意攻擊，以竊取使用者的隱私。因此許多研究人員極爲重視RFID隱私保護的問題，並提出許多的安全機制來保護RFID系統在通訊過程中資料的完整性與隱私性。

2. 背景、動機與目的

近年來，RFID系統被應用於各領域之中，爲我們的生活帶來許多的便利性，但也產生了許多資料的隱私安全問題。當RFID系統進行通訊傳輸的時候，過程中所包含資訊通常是個人隱私性的資料，因此有心人士只要在適當距離之間截取訊息，便可得知使用者相關的隱私訊息。近年來，許多學者相繼提出一些保護RFID隱私安全的通訊協定，在[4][5][6]所提出的RFID通訊協定中，以雜湊函數與隨機亂數爲主的安全機制，使讀取器每次收到標籤的訊息都不同，防止標籤暴露行蹤隱私而被攻擊者追蹤的安全性問題。

當RFID系統涉及到電子收費時，在交易過程中的隱私性與安全性是我們所關注的一個議題，所以本研究設計一個運用RFID系統之電子交易安全認證協定以保護使用者的隱私權益。

國道高速公路將於一〇二年全面實施電子計程收費，依據交通部高速公路局的規劃，將給予利用預付式及後付式不同繳費方式之用路人有不同之通行費費率。同時，希望透過費率實質差異，以鼓勵用路人使用最方便及有利方式繳交通行費。

高公局表示，國道預計於一〇二年實施ETC計程收費，屆時現有收費站將全面撤除，進入全面ETC計程收費後，部分未申裝ETC設備而使用高速公路用路人之繳費方式，將比照ETC用路人之欠費繳款模式，即使用高速公路後有自動繳費期，用路人可透過便利商店多媒體機器、網路及客服專線等方式查詢通行費應繳金額，並於各通路進行繳費。當逾自動繳費期時，再以郵寄方式寄送補繳通知單。

然而，用路人未申辦ETC雖然也可以行駛高速公路，於事後再行繳交通行費，但這種後付方式（事後繳費），容易發生忘記自動繳費、通知補繳時增加作業處理費用或衍生逾期未繳費之違規等情形，易對用路人產生困擾。因此，高公局特別依據高速公路不同使用類型用路人之需求，規劃多元繳費方式並搭配鼓勵措施。

遠通電收eTag爲被動式扣款設備（其原理與悠遊卡類似），屬RFID (射頻識別技術)之「預付式後處理」(Prepaid Post Process，簡稱：PPP)扣款設備，具有貼了即上路、免電池、無機無卡、下車免收機、預儲帳戶管理、無須IC 卡記錄儲值與交易金額等特性；預儲帳戶餘額不足，將發送欠費簡訊至用戶指定電話，提醒用戶於期限內主動補繳或補儲值。惟若超過自動補繳期，將依規定寄送繳款通知單，每筆欠費皆需加收作業處理費，若用路人未於繳款通知單所載繳款期限內完成補繳，仍會有逾期罰單舉發。

針對目前國內高速公路的收費運行模式，存在以下幾點問題：

1. 國內高速公路現階段計費方式仍需以收費站數量來進行付費，計次付費方式是不論走多少路程經過收費站就得付費，此方式對大多數駕駛人較爲不公平。且目前高速公路收費方式大多以傳統人工來進行收費，以致駕駛人須事先購買回數票或自備零錢付費，此收費方式降低駕駛人的便利性。
2. 高速公路現行之電子收費系統，駕駛人必須於上路前預先在「易通卡」儲存足夠的扣款金額以供實際扣款之用，此收費方式爲預付方式；假設駕駛人沒注意到「易通卡」儲值金額不足而經過收費站以致無法進行扣款，將導致駕駛人被罰款。

在這資訊科技發達的社會，每個人都具備有一個(含)以上的行動通訊裝置設備，爲了因應這股科技潮流，本系統架構假設於一個無線網路爲基礎的環境底下，結合應用RFID系統與行動通訊裝置建構一個高速公路電子收費系統架構，改善現行國內高速公路電子收費系統與傳統人工收費模式之缺失，提供駕駛人使用電子付費之交易安全性，以達到：

1. 安全、便利及公平的電子收費系統，降低人力成本，達到計費合理化與便利性。
2. 管理駕駛人行駛高速公路之認證及計費服務，並達到交易安全性及隱私權保護。

二、文獻探討

近年來，RFID應用在各領域上越趨成熟。RFID技術是一種裝置在物品上的標籤，以記錄該物品相關資料，優點在於Reader可以在任何角度讀取資料及同時讀取多張Tag，並擁有隨時更新資料的特性。RFID應用範圍十分廣泛，爲人們帶來自動化與高效

率效益，其中幾種常見應用領域包含人員身分辨識、門禁管理、物品追蹤、圖書管理系統、電子交易等，減少人力支出，以降低整體成本。

RFID系統較大的問題點在於資料隱私的問題。RFID系統能夠同時讀取多個標籤，可快速辨識標籤資訊，但RFID系統是透過無線電波來進行無線傳輸接收訊息，容易遭受有心人士攻擊與破壞，面臨使用者隱私權安全議題，因此一個安全的RFID認證協定，必須滿足下列安全性需求[7][8]：

- 行蹤隱私：
  因爲標籤記錄著唯一的識別資訊，攻擊者可藉由此識別資訊追蹤標籤位置，侵犯使用者行蹤隱私，所以標籤身分必須以密文來傳送，即使攻擊者攔截某標籤訊息，也無法利用此訊息來得知此標籤行蹤動向。
- 隱私保護性：
  標籤資訊在傳送過程中是必須被加密保護的，傳輸的資訊當中包含了標籤的辨識資料與使用者的一些隱私資料。所以標籤必須要能抵抗攻擊者攔截某標籤訊息，攻擊著也無法將此標籤訊息破解，竊取使用者相關隱私訊息。
- 資料完整性：
  標籤有重複寫入的特性，攻擊者在雙方認證過程中造成資料錯誤，導致雙方所儲存的資訊不同，因此認證機制必須能抵擋攻擊者的行爲，保持標籤資料在雙方的完整性。即使標籤訊息遭受到有心人士修改內存訊息，系統還是能正確讀取標籤訊息。
- 抵抗重送攻擊：
  攻擊者在傳輸過程中監聽某次的傳送訊息，並且在下一次通訊時，傳送相同的訊息給合法角色驗證，合法的讀取器會將攻擊者判斷爲合法的，攻擊者即可每次傳送相同的訊息給合法讀取器，使得合法讀取器允許被攻擊者追蹤。故認證機制必須要讓攻擊者攔截標籤訊息之後，亦無法將此訊息以重送方式來欺騙後端資料庫。
- 抵抗僞造攻擊：
  即使攻擊者竊取某標籤訊息，也無法將此訊息僞造成合法標籤來欺騙讀取器。
- 抵抗阻斷服務攻擊：
  即使攻擊者將無線通訊中斷或造成癱瘓行爲，系統也能正確執行辨識標籤的動作。
- 向前安全性：
  即使攻擊者破解某一標籤訊息及機密通訊資訊，亦無法將收集到的歷史訊息進行分析，向前追蹤此標籤過去的通訊信息。

1. RFID非密碼學保護機制

- **標籤刪除(Kill Tag approach)**

爲了保護使用者隱私，最簡單的方式，就是直接將標籤內所存放的所有資訊刪除。雖然Kill 功能可以將標籤內的資料徹底刪除，但標籤資料遭到刪除後，標籤就無法繼續使用，所以Kill 功能具有足夠的安全性，但也限制了電子標籤可重複使用的範圍[9][10]。

- **阻斷標籤(Blocker Tag)**

模擬所有標籤的識別碼，做一個阻斷標籤資訊的干擾標籤，擾亂商品本身的識別碼，讓攻擊者無法辨識使用者持有產品真正的識別碼[11][12]。2004年，RSA Security公

司在一場會議中展示了RSA Blocker Tag這項技術，商店將提供一個裝置RSA Blocker Tag技術的購物袋給消費者，以阻斷購物袋裡的資料防止RFID讀取器讀取，如果將商品放進此購物袋裡，讀取器就無法讀取袋中的商品資訊，若消費者將商品於袋中取出，商品就無法受到保護而被讀取器取得資訊。

- **識別碼分離(Physical ID Separation)**

將標籤識別碼分爲兩個部分，一個爲存有產品類別的識別碼(Class ID)，另一個爲產品數值的識別碼(Pure ID)。當產品賣出時將Class ID更換爲另一組新的Class ID，讓產品資訊無法被辨識[13]。

2、RFID密碼學保護機制

- **Hash Based Access Control**

2003年，Weis et al.提出以雜湊函數爲基礎的認證機制[4]，使用被動式標籤，假設標籤存在於不安全通道，讀取器與後端資料庫爲安全通道，標籤可能遭受攻擊，因此攻擊者能夠獲得標籤裡所存放的重要訊息。

下圖2.1爲Hash Based Access Control機制通訊過程。

圖2.1： Hash Based Access Control機制圖

此機制於傳輸過程中，在標籤身分辨識碼未更改的情況下，很容易被惡意的攻擊者辨別而追蹤；讀取器與標籤之間傳送之key值，若遭到攻擊者竊取將可解開標籤上鎖狀態，此機制雖然計算量低，但也存在幾項安全性上的疑慮。

(1)轉換 ID 可能會遭受攻擊者進行重送攻擊。

(2)轉換 ID 固定不變，攻擊者便能追蹤標籤使用情形。

- **Hash Chain**

Ohkubo et al.提出了以雜湊鏈爲主的認證機制[5][14]，假設標籤存在於不安全通道，讀取器與後端資料庫爲安全通道。此機制在每一個標籤會儲存各自的私密值，並在資料庫上存放每一個標籤的標籤識別碼及所對應的私密值。此機制透過Hash Chain更新私密值，以達到不可追蹤性。此機制亦提供向前安全的功能，當標籤被竊聽後，它的私密值會被攻擊者截取，但攻擊者無法於同一標籤去追蹤先前的資訊。

此認證機制雖能達成隱匿性及向前安全性，卻忽略了重送攻擊的安全性。

- **Hash-based Varying identifier**

2004 年，Henrici和Muller 提出了能夠達到資料保密和位置隱私的安全認證機制[15][16]，此機制利用標籤識別碼可變換的特性，來達到隱私、不可追蹤的特性。標籤存在於不安全通道，讀取器與後端資料庫爲安全通道。此機制運用更新識別碼ID_ x來避免標籤被追蹤的可能性，將同一標籤儲存新與舊兩筆記錄以防止阻斷攻擊。

此機制在2004年被指出無法達到不可追蹤性[17]，若在標籤識別碼更新過程中發生中斷現象，標籤識別碼便不會改變，所以只要標籤識別碼在沒有更新的情況下，就無法達成不可追蹤性。

- **Symmetrical Secret Key Cryptography**

2004年，Feldhofer et al.提出使用AES的安全認證機制[17]，提供RFID系統較高層級的安全性。想將訊息M從來源端A傳送至目的地端B，在傳送M之前，必須先利用A與B的共享金鑰K來進行加密。

此機制所需的硬體資源並不適合目前低成本的被動式標籤，且也不具備向前安全的特性。

- **Randomized Access Control**

由於Weis et al.所提出的Hash Based Access Control機制無法達到不可追蹤性，因此，Rhee等學者後續又提出Randomized Access Control機制[6]，以達到不可追蹤性。與Hash Based Access Control機制同樣以雜湊函數加密外，增加了亂數產生器。當標籤收到詢問訊息時，將隨機產生一個亂數值R及計算訊息傳送出去，讀取器必須向後端資料庫請求搜尋所有標籤識別ID，再將所收到的R值進行hash計算，與收到的訊息進行比對，若相同則爲合法標籤。

Weis et al.將標籤與資料庫存有一把私密金鑰，將使此機制更加強壯。在通訊過程中，電子標籤識別碼未更改情況下，容易被攻擊者追蹤，或者後端資料庫資料未更新，只要複製電子標籤內儲存的資料，便可以僞造其標籤。此安全機制必須對後端資料庫裡的所有資料進行搜尋或運算的動作（暴力破解方式，brute force），對後端資料庫是一項不小的負擔。此機制兼具以下特性與問題：

1. 改善轉換ID不變的特性，加入隨機亂數機制來改變每次傳輸的訊息，讓攻擊者無法追蹤標籤當下使用情形。
2. 依舊會遭受重送攻擊，藉以欺騙合法讀取器。
3. 標籤識別碼由讀取器直接傳送未更新的識別碼至標籤，造成了安全性上的缺失。

此機制雖能達到不可追蹤性，但與Hash Based Access Control 機制可能遭受攻擊者利用重送方式進行攻擊。

- **Challenge-Response based RFID Protocol**

2005年，Rhee et al.提出了一個簡單的認證機制[6]，同樣是利用雜湊函數與隨機亂數進行運算。將每個標籤儲存不同的亂數值ID，在後端資料庫存放每個標籤ID與相關資訊。

讀取器將隨機產生一個亂數a值發送至標籤，標籤收到訊息之後將產生一個亂數b值進行計算，標籤將所計算後的訊息與b值一同傳送至讀取器，讀取器將所收到的訊息與a值一起轉送至後端資料庫，資料庫收到訊息之後將所存放的ID值與a與b值進行hash計算，將所計算後數值進行比對，直到比對出相同的數值爲止。

此機制具備不可追蹤的特性與避免被惡意欺騙的攻擊，並能達到雙向認證，但不具有向前安全的特性，一旦標籤訊息被截取造成歷史訊息的洩漏，攻擊者便能追蹤歷史訊息。

上述幾項RFID安全認證機制，無法有效提供RFID系統完整的隱私保護，且通訊過程中皆需大量計算來進行驗證，並不適合低成本標籤使用。所以無法達到高安全性與低成本的雙重要求。

三、結合RFID之高速公路電子收費系統的認證與隱私權的保護系統

本研究所建構的電子收費系統架構，主要是運用RFID系統認證協定架構出合理收費兼具隱私安全的電子收費協定。以下說明電子收費架構。

一、系統架構

本節將提出結合RFID系統於電子收費所架構之安全認證協定，如圖3.1所示，本系統以RFID安全認證協定爲基礎，應用於高速公路電子收費機制。

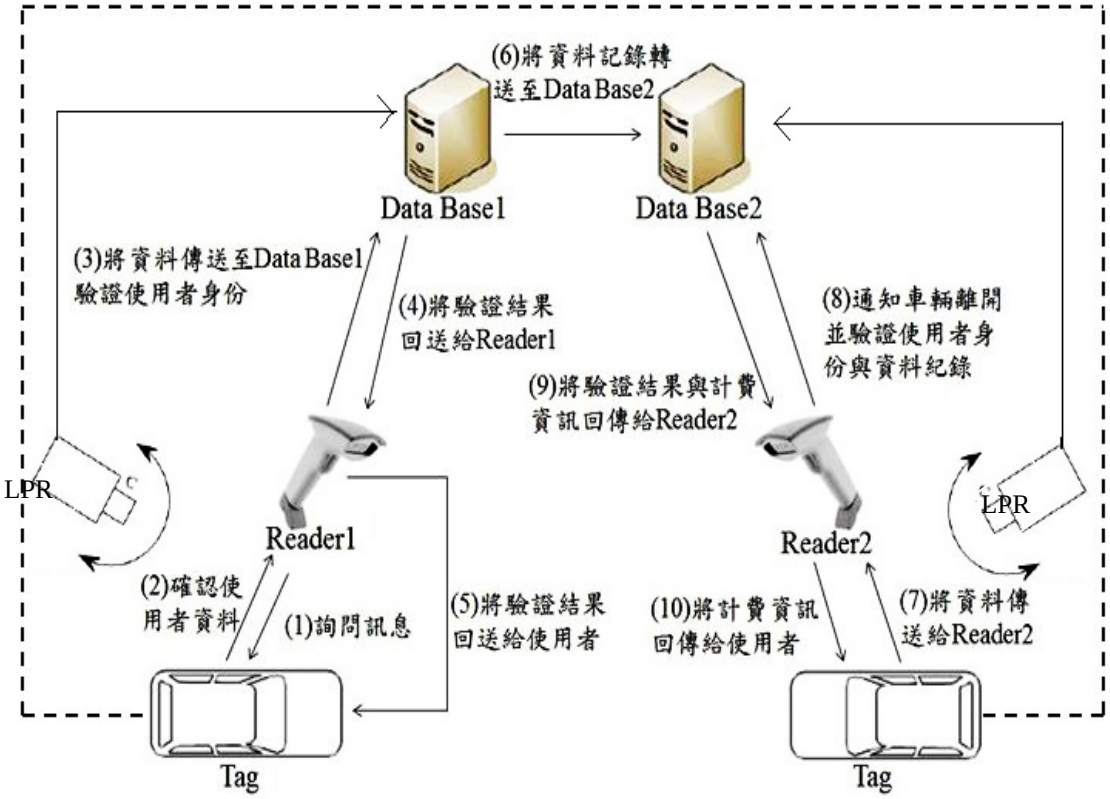

圖3.1：高速公路電子收費系統架構圖

下列爲本架構之步驟說明：

- **進入高速公路**

1. Reader1 → Tag：宣告
   當車輛(Tag)移動，進入Reader1通訊範圍內，Reader1就會發出廣播訊息，請車輛進行資料驗證。
2. Tag → Reader：資料傳送
   當車輛接收到廣播訊息後，車輛傳送的資料訊息須包含車輛基本資料、駕駛人行動設備所預設駕駛資訊。
3. Reader1 → DataBase1：資料驗證

當車輛進入匝道口時，Reader1將所記錄的車輛基本資料、進入時間與地點，此使用者基本資料訊息傳送至DataBase1，車牌辨識系統會把偵測到的車牌資訊傳送至DataBase1，此步驟是爲了防止駕駛人故意不使用Tag上路，將資訊存檔於DataBase以供日後發生繳費糾紛，以供查詢用。當DataBase1接收到訊息之後，會立即對使用者身分及車輛資料進行比對動作，當比對通過即執行下一步驟；若比對失敗將退回驗證資料並通知國道警察。

4. DataBase1 → Reader1：驗證結果
   此步驟是將資料驗證結果傳送至Raeder1
5. Reader1 → Tag：紀錄驗證資料
   當Reader1收到驗證成功之資料後即轉傳至Tag，Tag將此相關訊息紀錄以供計費之用。
6. DataBase1 → DataBase2：資料記錄轉傳
   DataBase1將所記錄的相關驗證資料轉傳至DataBase2以供計費之用。

● **離開高速公路**

7. Tag → Reader2：資料傳送
   當車輛駛離高速公路，Tag移動至Reader2通訊範圍內，Reader2將發送通訊需求，車輛傳送的資訊需包含車輛基本資料、進入時間與地點。
8. Reader2 → DataBase2：資料驗證
   當車輛準備離開匝道口時，由Reader2將此使用者基本資料訊息傳送至DataBase2，車牌辨識系統會把偵測到的車牌資訊傳送至DataBase2，記錄的車牌相關基本資料，由系統紀錄離開時間與地點，當DataBase2接收到訊息之後，會立即對使用者身分及車輛資料進行比對動作，當比對通過即計算車輛所行駛之里程數費用。
9. DataBase2 → Reader2：計費資訊
   此步驟是將上步驟之計算結果傳送至Reader2，也將傳送訊息至使用者行動通訊設備以告知此趟路程付費相關資訊。
10. Reader2 → Tag：
    當Reader2收到計算結果後即轉傳至Tag，並告知Tag已使用完畢。

二、本系統符號說明

以下爲通訊協定相關符號：

- Tag內存欄位
  L：Tag ID的雜湊數值
  DK：DataBase與Tag的共享金鑰
- Reader內存欄位
  RID：Reader識別ID
  RK：DataBase與Reader的共享金鑰
  Data：時間、地點
- DataBase內存欄位

Tag ID：於DataBase存放各Tag ID

RID：Reader識別ID

DK：DataBase與Tag的共享金鑰

RK：DataBase與Reader的共享金鑰

三、系統運作階段

- **進入高速公路**

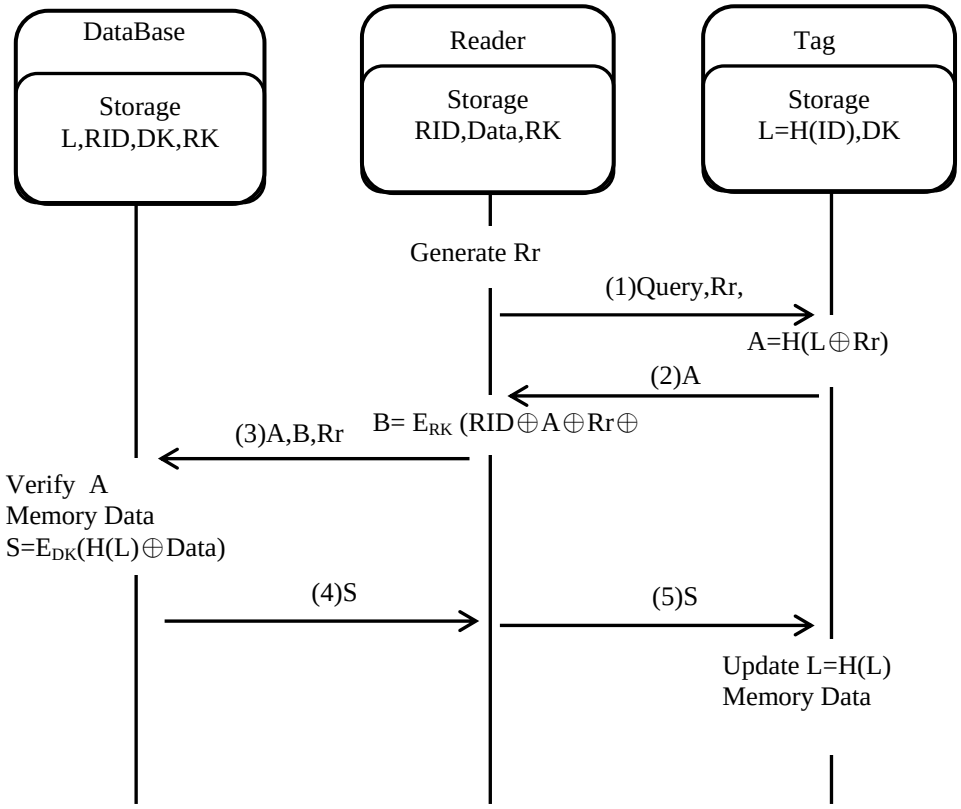

圖3.2： 進入高速公路系統認證協定圖

步驟說明：

1. Reader → Tag：Reader將Query與所產生的亂數Rr傳給Tag，做爲讀取要求。
2. Tag → Reader：Tag在收到Rr後，Tag會將內存已加密過的標籤識別碼L=H(ID)與Rr進行計算A=H(L⊕Rr)，並將所計算出的A值傳送至Reader。
3. Reader → DataBase：當Reader接收到A後，便利用讀取器識別碼RID、所產生的亂數Rr與車輛進入高速公路之時間地點資訊Data進行運算，得到B=ERK(RID⊕A⊕Rr⊕Data)的數值，Reader將A、B與Rr傳送至Data Base。
4. DataBase → Reader：DataBase收到Rr後，便利用DataBase內存放的ID值做計算，並比對Reader所傳送的A值是否相同，若不相同則中斷連線，數值相同即爲合法訊息將接續以RID、A及Rr與B進行運算，即可得知進入高速公路資訊Data，隨即將Data資訊存放於資料庫以供計費之用，並將L更新爲H(L)儲存於資料庫，資料庫將與Tag共享金鑰DK進行運算S= EDK(H(L)⊕Data)，資料庫將行車資訊S傳送至Reader。
5. Reader → Tag：當Reader收到行車資訊S之後，將此訊息S轉傳至Tag。當Tag收到

S後，便利用與DataBase所共享的金鑰DK解開S訊息，進行XOR運算得到H(L)及獲得Data，Tag將L更新爲二次加密的H(L)、Data儲存於Tag以完成進入高速公路的資料認證程序。

- **離開高速公路**

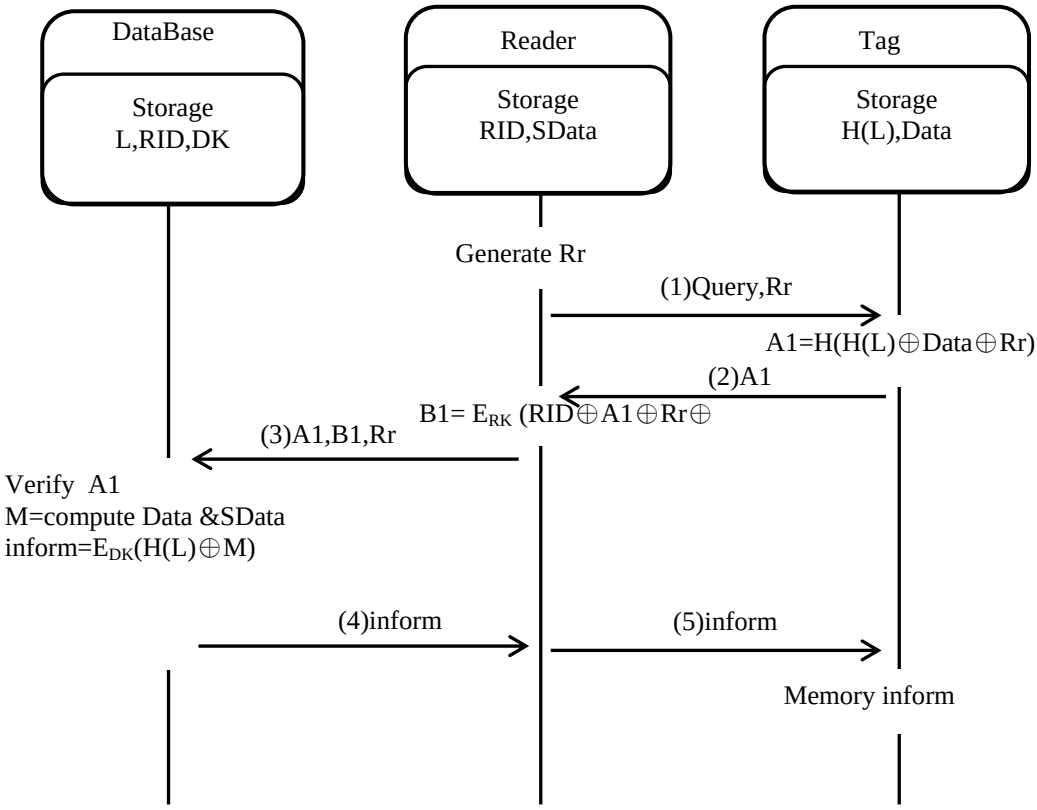

圖3.3：離開高速公路系統認證協定圖

步驟說明：

6. Reader → Tag：Reader將Query與所產生的亂數Rr傳給Tag，做爲讀取要求。
7. Tag→ Reader：Tag在收到Rr後，將所收到的Rr與標籤識別碼H(L)，計算出A1=H(H(L)⊕Data⊕Rr)，並將所計算出的A1值傳送至Reader。
8. Reader → DataBase：當Reader接收到A1之後，將讀取器識別碼RID、亂數Rr與車輛離開高速公路之時間地點資訊SData進行運算，得到B1= ERK (RID⊕A⊕Rr⊕SData)的數值，Reader將A1、B1與Rr傳送至Data Base。
9. DataBase → Reader：DataBase收到的Rr之後，便使用DataBase所存放的H(L)值做計算，並比對所接收的A1值是否相同，若不相同則中斷連線，數值相同即爲合法訊息將接續以RID、A1及Rr與B1進行運算，即可得出離開高速公路資訊SData，隨即計算Data與SData得出計費資訊M，資料庫將與Tag共享金鑰DK進行運算inform= EDK(H(L)⊕M)，資料庫將路程計費資訊inform傳送至Reader。
10. Reader → Tag：當Reader收到計費資訊inform之後，將此訊息inform轉傳至Tag。當Tag收到inform後，便利用與DataBase的共享金鑰DK解開inform訊息，進行XOR運算得到行車資訊M。

四、安全性與效能比較分析

由於本系統利用RFID系統結合電子收費,所以安全議題隨著許多相關運用發展而使得在隱私安全方面更加的需要被重視，其中資料傳輸安全防護、個人隱私保護是RFID運用的重要考量之議題。因此本系統使用簡單的互斥或(XOR)、雜湊函數(Hash Function)運算、隨機亂數機制 (Randomize Mechanism)與祕密金鑰加密機制(Secret Key Encryption Mechanism)來建構出一個具隱私保護的雙向鑑別機制，可適用於計算能力弱、記憶體容量小的被動式Tag中，以提供Tag與Reader間安全的雙向鑑別管道，於此章節將分別對本研究所提出之電子收費架構與現行收費方式做一比較分析,與本系統所具備的安全性優勢。

1. 安全性分析

本系統通訊協定具行蹤隱私、預防重送攻擊、預防訊息竊取、預防阻斷服務攻擊及向前安全，說明如下：

◆ 行蹤隱私

本研究並不會將Tag ID 以明文方式傳送，而是利用雜湊函數保護，在通訊過程當中L值也不會以明文方式來傳送，而是利用XOR及雜湊函數加以保護，故可避免雜湊鍊方式反追蹤，防止惡意人士對Tag進行追蹤行爲。

◆ 重送攻擊

Reader在每次通訊時，隨機產生一個亂數Rr以保護傳輸資料，確保該次通訊的機密性避免重送攻擊。

◆ 訊息竊取

通訊過程中所傳送的訊息是採XOR、雜湊函數來保護，且每次驗證亂數皆爲隨機產生，故每次認證結束訊息也會更新，防止惡意人士竊取機密資訊。

◆ 阻斷服務攻擊

本研究在驗證通過的話，就會將該次認證訊息進行更新，防止惡意人士以阻斷服務資料更新的方式造成系統資料不一致問題。

◆ 向前安全

通訊過程中使用雜湊函數進行保護，每次產生的訊息也會不同，當攻擊者攔截通訊資料後，破解Tag 在某個時間點的訊息，也無法向前追溯歷史訊息。

本系統於匝道處架設車牌辨識系統，主要目的是與RFID系統互相搭配，達到雙重驗證功效，以防止有心駕駛人利用金屬材質物品阻斷Tag感應，而無法進行里程計費。搭配車牌辨識系統，車道控制器內的影像處理將通過匝道口之車輛車牌圖像與車牌號碼加以分析與辨識，將所擷取的車輛相關影像資訊於車道控制器中建檔儲存，此相關資訊可於日後產生爭議時，以供相關單位查詢罰緩。本研究所架構的交易系統是與無線行動裝置做結合，當車子進入感測範圍內，系統立即向車載單元要求行駛所需登入的基本資料，以記錄範圍內的使用者，而通過匝道時，系統將記錄駕駛人基本資料與車牌資料，利用此雙重記錄以提高付費的安全性。本系統不像現有電子收費系統(ETC)，只要盜取

其他駕駛人的E通卡即可進行付費。由於本架構配有行車監控系統，所以當車子遭竊或發生違規事件，可立即搜尋車子行蹤。下表4.1說明本系統架構與現行收費機制在付費安全性、防止竊盜事件、違規取締皆比現階段所使用的人工收費方式與電子收費系統較具安全性與便利性。

表4.1： 電子收費系統之安全性分析表

	人工收費方式	ETC電子收費系統	本系統
付費安全性	較高	較低	較高
是否降低竊車事件	否	否	是 (可追蹤車輛資訊)
是否能立即取締 違規事件	否	否	是
個人行程隱私	較高	較高	較高

2. 效能比較

本架構付款機制是結合電信業者於行動裝置的每月帳單中，採用後付機制，且於每次消費後系統會自動發送消費訊息至使用者的行動裝置，此方式可讓使用者清楚自己的消費情況，且採用月結方式與手機帳單一起繳費即可。反之現行ETC系統須採用預先儲值方式，如駕駛人沒注意到預儲金額不足而行經收費站，則會產生扣款不足情形發生而遭罰款。在路程計費部分，本架構是以行駛多少路程就付與多少費用，以行駛里程數來進行計費，使用者付費更爲合理，不像目前收費模式皆在固定收費匝道，只要經過收費站就必須進行付費較不公平合理。於收費匝道裡車輛回堵問題，因車輛必須減速進行付款動作，這樣易造成匝道車流變慢與回堵情形發生，且無法計算車流量，但本系統匝道偵測設置於交流道，在使用上較爲便利，行車時較不易造成回堵，也不需較低車速。下表4.2說明本系統架構與現有高速公路電子收費系統之效能分析。

綜合以上安全性與效能比較，目前現行之電子收費系統(ETC)只是將一般人工收費方式轉變爲電子化。而本架構提出的電子收費系統不僅考量到電子交易之安全性，也降低了人力成本，在安全性及效率上均比目前國內高速公路的人工收費及現有電子收費系統(ETC)擁有較多優點。最終以達到具安全、便利、公平爲原則之電子收費架構。

由於本系統架構提出的付費機制是結合電話帳單以月結方式付款，即爲先使用後付費，此付款模式有可能造成呆帳問題，如：使用者刻意不付費、忘記繳費…等，故建議與電信業者在一個月以上未繳款的使用者進行停話與加值服務的使用，希望以此方式來提醒使用者進行付款。其實eTag預付型亦會有預儲帳戶餘額不足之問題，本機制亦可比照etag模式將發送欠費簡訊至用戶指定電話，提醒用戶於期限內主動補繳，惟若超過自動補繳期，將依規定寄送繳款通知單，每筆欠費皆需加收作業處理費，若用路人未於繳款通知單所載繳款期限內完成補繳，仍會有逾期罰單舉發。

表4.2： 高速公路電子收費系統之效能分析表

	人工收費方式	ETC電子收費系統	本系統
付款機制	先付(購買回數票)	先付(儲值)	後付(並收到計費訊息)
付款便利性	不便 (須特定地點購買)	不便 (須特定地點儲值)	方便(與電話帳單一起繳交)
能否以里程計費	否	否	能
車輛辨識處	收費站	收費站	匝道管制口
車流狀況	易阻塞	易阻塞	不易阻塞
車流速度	車速較慢	車速較慢	車速較快
人力成本	高	低	低
車流量計算	人工計算	系統計算	系統計算
缺點	人爲疏忽	須以預付方式付款	易造成呆帳

伍、結論

由於資訊時代的發展快速，並鑑於目前國內高速公路收費機制系統的不便與缺失，本論文結合RFID系統與高速公路電子收費系統，架構出一套適用於高速公路電子收費的認證與隱私權保護系統，目的在於提供使用者一個更加安全、便利與完善的電子交易環境。整個電子交易過程可以有效且清楚的記錄駕駛人交易資料，並將費用以月結的方式結合於每月的行動通訊裝置帳單，駕駛人在上路前不必事先花費時間購買回數票或將易通卡儲值。此系統架構應用於高速公路上，可大幅提升駕駛人使用的便利性，並讓以次計費的機制改爲較公平的里程計費。

[謝啓]

本刊承蒙國科會提供計畫經費補助(計畫編號：NSC 101-2221-E-218 -052)，特此致謝。

參考文獻

[1] Nath, B., Reynolds, F. and Want, R., "RFID Technology and Applications", *IEEE Pervasive Computing*, January/ March, 2006.

[2] Garfinkel, S. L., Juels, A. and Pappu, R., "RFID privacy: an overview of problems and proposed solutions", *IEEE Security and Privacy*, 2005: pp.34-43.

[3] Phillips, T., Karygiannis, T. and kuhn, R., "Security Standards for the RFID Market", *IEEE Security and Privacy*, 2005: pp.85-89.

[4] Weis, S. A., Sarma, S. E., Rivest, R. L., and Engels, D. W., "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems", *Security in Pervasive Computing*, 2003: pp.201-212.

[5] Ohkubo, M., Suzuki, K. and Kinoshita, S., "Cryptographic Approach to Privacy-friendly Tags", *RFID Privacy Workshop*, MIT, MA, USA, Nov 2003.

[6] Rhee, K., Kwak, J. and Kim, S., "Challenge-response based RFID authentication protocol for distributed database environment", *International Conference on Security in Pervasive Computing*,

2005: pp.70-84.

[7] Shih, D. H., Lin, C.Y. and Lin, B., "RFID Tags: Privacy and Security Aspects", *International Journal of Mobile Communications*, Vol. 3, No. 3, 2005: pp.214-230.

[8] Wang, S. and Wang, F., "Security Analysis of Some RFID Authentication Protocols", *e-Business and Information System Security (EBISS)*, 2010 *2nd International Conference*, May 2010: pp.22-23.

[9] Juels,A., "RFID Security and Privacy: A Research Survey", *IEEE Journal on Selected Areas in Communications*, Vol. 24, 2006: pp.381-394.

[10] Kim, I. J., Choi, E. Y., and Lee, D. H.. "Secure Mobile RFID system against privacy and security problems", *Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, 2007: pp.67-72.

[11] Juels, A., Szydlo , M., and Rivest, R. L., "The Block Tag: Selective Blocking of RFID Tags", *ACM Consumer Privacy*, May 2003: pp.103-111.

[12] Juels, A., "Strengthening EPC Tag against Cloning", To Appear in the *Procceedings of WiSe*, 2005.

[13] Inoue, S. and Yasuura, H., "RFID Privacy Using User-controllable Uniqueness", *RFID Privacy Workshop*, MIT, 2003.

[14] Zhang, Y. L. and Guo, H., "An Improved RFID Privacy Protection Scheme Based on Hash-Chain", *Logistics Engineering and Intelligent Transportation Systems (LEITS)*, 2010 International Conference, Nov. 2010: pp.26-28.

[15] Henrici, A. D., and Muller, P., "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers", In the *Proceedings of PerSec'04 at IEEE PerCom*, 2004: pp.149-153.

[16] Mohabbat, H., "Authentication and Lightweight Cryptography in Low Cost RFID", *Software Technology and Engineering, 2nd International Conference*, 2010: PP. V2-123 - V2-129.

[17] Feldhofer, M., Dominikus, S., and Wolkerstorfer, J., "Strong Authentication for RFID Systems Using the AES Algorithm", *proceedings of the CHES* ' 04, LNCS vol. 3156, 2004: pp. 357-370.